EDOK - Application for Search Warrant (Revised 5/13)

United States District Court

EASTERN DISTRICT OF OKLAHOMA

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH FACEBOOK USER ID SAUL.FRIAS.14; THAT IS STORED AT PREMISES CONTROLLED BY FACEBOOK INC.	Case No. MJ-16-031-KEW

APPLICATION FOR SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that there is now concealed on the following person or property located in the Northern District of California *(identify the person or describe property to be searched and give its location)*:

SEE ATTACHMENT "A"

The person or property to be searched, described above, is believed to conceal *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT "B"

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of Title 18, United States Code, Sections 2251, 2252A and 2422(b), and the application is based on these facts:

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Jonathan Clark
Special Agent
Federal Bureau of Investigation

Sworn to before me and signed in my presence.

Date: May 11, 2016

City and state: Muskogee, Oklahoma

Judge's signature

KIMBERLY E. WEST
UNITED STATES MAGISTRATE JUDGE
Printed name and title

ATTACHMENT "A"

DESCRIPTION OF PROPERTY TO BE SEARCHED

This warrant applies to information associated with the following Facebook account: Saul Frias (saul.frias.14), that is stored at premises owned, maintained, controlled, or operated by Facebook, Inc. in Menlo Park, California.

ATTACHMENT "B"

INFORMATION TO BE SEIZED

I. Information to be disclosed by Facebook

To the extent that the information described in Attachment "A" is within the possession, custody, or control of Facebook, including any messages, records, files, logs, or information that have been deleted but are still available to Facebook, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Facebook is required to disclose the following information to the government for the user ID listed in Attachment A:

a. All contact, personal identifying information and stored account information, including full name, user identification number, birth date, gender, contact email address, Facebook passwords, Facebook security questions and answers, physical address (including city, state, and zip code), telephone numbers, screen names, websites, account status history, about me page, active sessions, alternate name, check-ins, connections, credit cards, current city, deleted friends, emails, followers, friend requests, friends, groups, IP addresses, last location, linked accounts, logins, logouts, messages, name changes, pending friend requests, phone numbers, photos, posts, recent activities, removed friends, searches, shares and videos and other personal identifiers.

b. All associated users and their Facebook ID's (associated means here every user that has logged into a Facebook account utilizing a username, machine, device, computer, web browser or any other electronic information or device) used by saul.frias.14 or Gmail address simonsantana59@gmail.com.

c. All activity logs for the account and all other documents showing the user's posts and other Facebook activities.

d. All photos and videos uploaded by that user ID and all photos and videos uploaded by any user that has that user tagged.

e. All profile information; news feed information; status updates; links to videos, photos, articles, and other items; notes, wall postings; friend lists, including the friends' Facebook user ID; groups and networks of which the user is a member, including the groups' Facebook group ID; future and past even postings; rejected "Friend" request; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications.

f. All other records of communications and messages made or received by the user,

including all private messages, chat history, video calling history, and pending "Friend" requests.

g. All "check ins" and other location information

h. All IP logs, including all records of the IP address logged into the account.

i. All records of the account's usage of the "like" feature, including all Facebook posts and all non-Facebook web pages and content that the user has "liked."

j. All information about the Facebook pages that the account is or was a "fan" of.

k. All past and present lists of friends created by the account.

l. All records of Facebook searches performed by the account.

m. All information about the user's access and use of Facebook Marketplace.

n. The types of services utilized by the user.

o. The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number).

p. All privacy settings and other account settings, including privacy settings for individual Facebook posts and activities, and all records shoring which Facebook users have been blocked by the account.

q. All records pertaining to communications between Facebook and any person regarding the user or the user's Facebook account, including contacts with support services and records of actions taken.

II. Information to be seized by the Government

All information described about in Section I that constitutes fruits, evidence and instrumentalities of violations of 18 U.S.C. §§ 2251(a) and 2251(d); 18 U.S.C. §§ 2252A(a)(2)(A), 2252A(a)(5)(B) and 2422(b) involving the above mentioned Facebook account including for the user ID identified on Attachment "A", information pertaining to the following matters:

a. Records regarding the production, distribution and possession of child pornography, and the coercion and enticement of a minor. This includes communications from this Facebook account, including all private messages and images contained within and records relating to who created, used, or communicated with the user ID, including records about their identities and whereabouts.

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

INTRODUCTION

I, Jonathan Clark, having been first duly sworn, do hereby depose and state as follows:

1. I make this affidavit in support of an application for a search warrant for information associated with a certain Facebook user ID that is stored at premises owned, maintained, controlled, or operated by Facebook Inc. ("Facebook"), a social networking company headquartered in Menlo Park, California. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Facebook to disclose to the government records and other information in its possession, pertaining to the subscriber or customer associated with the **User ID SAUL.FRIAS.14**.

2. I have been employed as a Special Agent of the FBI since 2008, and am currently assigned to the Ardmore Resident Agency of the Oklahoma City Division. While employed by the FBI, I have investigated federal criminal violations related to high technology or cyber crime, child exploitation, and child pornography. I have gained experience through new agent training at Quantico, Virginia, Internet Crimes Against Children training in Atlanta, Georgia, and everyday work relating to conducting these types of investigations. I have received training in the area of child pornography and child exploitation and have had the opportunity to observe and review examples of child pornography (as defined in 18 U.S.C. § 2256). Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal laws, including 18 U.S.C. §§ 2251, 2252A and 2422 and I am authorized by the Attorney General to request a search warrant.

3. In my training and experience, I have learned that Facebook Inc. is a company that operates a social network at Facebook.com, and that stored electronic communications at Facebook Inc. may include "Basic Subscriber Information" (BSI); "User Neoprint" information, which may include, but is not limited to, "Profile Contact Information," "Status Update History," "Notes," Wall Postings," and "Friends Listing"; "User Photoprint" information, which is a compilation of all photos uploaded by the user that have not been deleted; and, "Private Messages". Facebook subscribers may be located on the computers of Facebook Inc. which is located in California. Accordingly, this affidavit and application for search warrant seeks authorization solely to search the computer account and/or files following the procedures described herein.

4. I have probable cause to believe that contraband and evidence of a crime, fruits of a crime, and instrumentalities of violations of 18 U.S.C. §§ 2251(a) and 2251(d) (enticement of a child and advertisement child pornography); 18 U.S.C. § 2252A(a)(2)(A) (receipt and distribution of child pornography); 18 U.S.C. §§ 2252A(a)(5)(B) and 2252A(b)(2) (possession of, knowing access, conspiracy to access, or attempted access with intent to view child pornography); and 18 U.S.C. § 2422(b) (coercion and enticement), are on the Facebook account "saul.frias.14", (hereinafter the "SUBJECT ACCOUNT"). I submit this application and affidavit in support of a search for information associated with the SUBJECT ACCOUNT that is stored at premises owned, maintained, controlled, or operated by Facebook Inc., a social media company headquartered in Menlo Park, California. The location and information to be searched are described in the following paragraphs and in Attachments A and B, which are incorporated herein by reference. I request authority to require Facebook to disclose to the government

records and other information in its possession, pertaining to the subscriber or customer associated with the SUBJECT ACCOUNT.

5. The statements contained in this affidavit are based in part on: information provided by FBI Special Agents; written reports about this and other investigations that I have received, directly or indirectly, from other law enforcement agents; information gathered from the service of Grand Jury subpoenas; independent investigation and analysis by FBI agents/analysts and computer forensic professionals; and my experience, training and background as a Special Agent with the FBI. Because this affidavit is being submitted for the limited purpose of securing authorization for the requested search warrant, I have not included each and every fact known to me concerning this investigation. Instead, I have set forth only the facts that I believe are necessary to establish the necessary foundation for the requested warrant.

RELEVANT STATUTES

6. This investigation concerns alleged violations of 18 U.S.C. §§ 2251(a) and 2251(d) (Enticement of a minor and advertising Child Pornography); 18 U.S.C. § 2252A(a)(2)(A), (Receipt, Transportation, and Distribution of Child Pornography); and 18 U.S.C. §§ 2252A(a)(5)(B) and 2252A(b)(2) (Possession and Access, or Attempted Access, with Intent to View Child Pornography), and 18 U.S.C. § 2422(b) (Coercion and Enticement).

a. 18 U.S.C. §§ 2251(a) and 2251(d) prohibits a person from knowingly conspiring to make, print or publish, or causing to be made, printed or published, any notice or advertisement seeking or offering: (A) to receive, exchange, buy, produce, display, distribute, or reproduce, any visual depiction, if the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such

visual depiction is of such conduct, or (B) participation in any act of sexually explicit conduct by or with any minor for the purpose of producing a visual depiction of such conduct;

b. 18 U.S.C. § 2252A(a)(2)(A) prohibits a person from knowingly receiving, distributing or conspiring to receive or distribute any child pornography or any material that contains child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer;

c. 18 U.S.C. § 2252A(a)(5)(B) prohibits a person from knowingly possessing or knowingly accessing with intent to view, or attempting to do so, any material that contains an image of child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer; and

d. 18 U.S.C. § 2422(b) prohibits a person from using the mail or any facility or means of interstate or foreign commerce, or within the special maritime and territorial jurisdiction of the United States to knowingly persuade, induce, entice, or coerce any individual who has not attained the age of 18 years, to engage in prostitution or any

sexual activity for which any person can be charged with a criminal offense, or attempt to do so.

BACKGROUND OF THE INVESTIGATION AND PROBABLE CAUSE

7. On or about March 29, 2016, Ardmore Oklahoma Police Department notified the Ardmore Office of the Oklahoma City Division of the FBI that the Ardmore Police were dispatched to a residence the night before where they spoke with the parents of an 11 year old female, Jane Doe (hereinafter referred to as JD1). JD1's father told the Ardmore Police that JD1 came to him scared because of Facebook messages she had been receiving from a person who she believed was a male. Ardmore Police Officers reviewed JD1's cellular phone and saw messages from a sender with the name of Saul Frias telling JD1 that if she did not have sex with his friends, he would send "the video" to all of her friends and everyone that he knew. JD1's father told one of the officers the last thing Saul Frias sent JD1 was a video of JD1 naked while she "played with herself."

8. On or about March 30, 2016, JD1's father was interviewed by the FBI. JD1's father provided the FBI JD1's cellular telephone and provided the FBI consent to search the phone. JD1's father told the FBI that on March 28, 2016, he became aware of threatening Facebook Messenger communications to his 11 year old daughter, JD1, from an unknown individual. The unknown individual was threatening to send naked photos of JD1 to JD1's Facebook friends. JD1's father then took his daughter's phone that she had been receiving the messages from the individual via the Facebook Messenger application and he sent the unknown individual from JD1's phone a message letting the unknown individual know that he was JD1's father and to he needed to stop sending messages to JD1. The unknown individual then sent a

naked picture or video of JD1 to JD1's phone and JD1's father received it. JD1's father contacted the Ardmore Police Department. Facebook Messenger is an application that allows users to send messages to one another via the internet utilizing a computer or a cellular phone with internet access.

9. On or about March 30, 2016, JD1 was interviewed by the FBI. JD1 told the FBI she received a friend request from someone going by the name of Saul Frias on Facebook in or about mid-March 2016. Shortly after becoming friends, the user of the Saul Frias Facebook account requested JD1 to send nude pictures of herself. JD1 told the FBI that she does not personally know the person using the Facebook profile Saul Frias. After JDI sent sexually explicit pictures of her masturbating to the SUBJECT ACCOUNT, the person using that profile threatened to send JD1's pictures to JD1's family and to a friend.

10. On or about April 8, 2016, a digital forensic examination was conducted on JD1's cellular phone. The Affiant was advised by the FBI Agent who reviewed the evidence on the cellular phone that the phone contained, among other things, a video of a nude female touching her genitalia. The female appeared to be JD1. The phone also contained Facebook Messenger data from Saul Frias.

11. On April 8, 2016, FBI Agents compared the picture associated with the Facebook Messenger data from Saul Frias on JD1's phone to the profile pictures on Facebook's website associated with user name Saul Frias. Agents discovered many Facebook users going by the name Saul Frias, but that the only profile on Facebook that had the same profile picture as that from the messages on JD1's phone was the SUBJECT ACCOUNT. Agents also noticed that the SUBJECT ACCOUNT profile showed that the user resides in Ardmore, Oklahoma.

12. On April 25, 2016, the Affiant obtained a Grand Jury subpoena and served the same to Facebook for subscriber information and registration IP address for the SUBJECT ACCOUNT. The IP address is a unique numerical address that is assigned to a specific internet service provider and can be useful to pinpoint when a specific user, or user's account, was using a specific internet provider.

13. On or about May 2, 2016, the Affiant received the Facebook subpoena results for the SUBJECT ACCOUNT. The results showed that the account was created on February 27, 2016 from IP address 104.4.15.65 and that the registration email address was simonsantana59@gmail.com.

14. On or about March 30, 2016, a preservation request was sent to Facebook Inc.

15. The Affiant believes that at all times that the aforementioned images were sent by JD1, she was located in Ardmore, Oklahoma.

16. When JD1's father received the aforementioned images, he was located in Ardmore, Oklahoma.

17. Facebook Messenger messages travel in interstate commerce.

BACKGROUND ON FACEBOOK

18. Facebook owns and operates a free-access social networking website of the same name that can be accessed at http://www.facebook.com. Facebook allows its users to establish accounts with Facebook, and users can then use their accounts to share written news, photographs, videos, and other information with other Facebook users, and sometimes with the general public.

19. Facebook asks users to provide basic contact and personal identifying information to Facebook, either during the registration process or thereafter. This information may include the user's full name, birth date, gender, contact email address, Facebook passwords, Facebook security questions and answers (for password retrieval), physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers. Facebook also assigns a user identification number to each account.

20. Facebook users may join one or more groups or networks to connect and interact with other users who are members of the same group or network. Facebook assigns a group identification number to each group. A Facebook user can also connect directly with individual Facebook users by sending each user a "Friend Request." If the recipient of a "Friend Request" accepts the request, then the two users will become "Friends" for purposes of Facebook and can exchange communications or view information about each other. Each Facebook user's account includes a list of that user's "Friends" and a "News feed," which highlights information about the user's "Friends," such as profile changes, upcoming events, and birthdays.

21. Facebook users can select different levels of privacy for the communications and information associated with their Facebook accounts. By adjusting these privacy settings, a Facebook user can make information available only to himself or herself, to particular Facebook users, or to anyone with access to the Internet, including people who are not Facebook users. Facebook accounts also include other account settings that users can adjust, for example, the types of notifications they receive from Facebook.

22. Facebook users can create profiles that include photographs, lists of personal interests, and other information. Facebook users can also post "status" updates about their

whereabouts and actions, as well as links to videos, photographs, articles, and other items available elsewhere on the Internet. A particular user's profile page also includes a "Wall," which is a space where the user and his or her "Friends" can post messages, attachments, and links that will typically be visible to anyone who can view the user's profile.

23. Facebook allows users to upload photos and videos. It also provides users the ability to "tag" (i.e., label) other Facebook users in a photo or video. When a user is tagged in a photo or video, he or she receives a notification of the tag and ta link to see the photo or video. For Facebook's purposes, the photos and videos associated with a user's account will include all photos and videos uploaded by that user that have not been deleted, as well as all photos and videos uploaded by any user that have that user tagged in them.

24. Facebook users can exchange private messages on Facebook with other users. These messages, which are similar to email messages, are sent to the recipient's "Inbox" on Facebook, which also stores copies of messages sent by the recipient, as well as other information. Facebook users can also put comments on the Facebook profiles of other users or on their own profiles. In addition, Facebook has a Chat feature that allows users to send and receive instant messages through Facebook. These chat communications are stored in the chat history for the account. Facebook also has a Video Calling feature, and although Facebook does not record the calls themselves, it does keep records of the date of each call.

25. Each Facebook account has an activity log, which is a list of the user's posts and other Facebook activities from the inception of the account to the present. The activity log includes stories and photos that the user has been tagged in, as well as connections made through

the account, such as "liking" a Facebook page or adding someone as a friend. The activity log is visible to the user but cannot be viewed by people who visit the user's Facebook page.

26. In addition to the applications described above, Facebook also provides its users with access to many other functionalities and applications on the Facebook platform.

27. Facebook uses the term "Neoprint" to describe an expanded view of a given user profile. The "Neoprint" for a given user can include the following information from the user's profile: profile contact information; news feed information; status updates; links to videos, photographs, articles, and other items; notes; wall posting; friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejecting "Friend" requests; comments; gifts; pokes; tags; and other information about the user's access and use of Facebook applications.

28. Facebook also retains Internet Protocol (IP) logs for a given user ID or IP address. These logs may contain information about the actions taken by the User ID or IP address on Facebook, including information about the type of action, the date and time of the action, and the user ID and IP address associated with the action. For example, if a user views a Facebook profile, that user's IP log would reflect the fact that the user viewed the profile, and would show when and from what IP address the user did so.

29. Social media providers and social networking providers like Facebook typically retain additional information about their users' accounts, such as information about the length of service, the types of service utilized, and the means and source of any payments associated with the service (including any credit card or bank account information). In some cases, Facebook

users may communicate directly with Facebook about issues relating to their accounts, such as technical problems, billing inquiries, or complains from other users. Social media providers like Facebook typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. Facebook stores its information on servers which are located in California. The information and data that is provided by the user is done so buy use of the internet using electronic media such as computers that access the internet or phones that access the internet. Therefore, the computers of Facebook are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Facebook, such as account access information, transaction information, and other information.

30. As explained herein, information stored in connection with a Facebook account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, a Facebook user's "Neoprint," IP log, stored electronic communications, and other data retained by Facebook, can indicate who has used or controlled the Facebook account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, profile contact information, private messaging logs, status updates, and tagged photos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the Facebook account at a relevant time. Further, Facebook account activity can show how and when the account was accessed or used.

For example, as described herein, Facebook logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Facebook access, use, and events relating to the crime under investigation. Additionally, Facebook builds geo-location into some of its services. Geo-location allows, for example, users to "tag" their location in posts and Facebook "friends" to locate each other. This geographic and timeline information may tend to either inculpate or exculpate the Facebook account owner. Last, Facebook account activity may provide relevant insight into the Facebook account owner's state of mind as it relates to the offense under investigation. For example, information on the Facebook account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement). Therefore, the computers of Facebook are likely to contain all the material described above, including stored electronic communications and information concerning subscribers and their use of Facebook, such as account access information, transaction information, and other account information.

SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

31. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Facebook to disclose to the government copies of the records and other information (including the content of communications) particularly described in Section I of Attachment B.

Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

32. The item that is the subject of the search is Facebook Account **saul.frias.14** controlled or operated by the social media site known as Facebook Inc., 1601 Willow Road, Menlo Park, CA 94025. As set forth herein, there is probable cause to believe that on the computer systems of Facebook, Inc., there is evidence of violations of 18 U.S.C. §§ 2251, 2252A and 2422(b). Specifically, the Facebook accounts mentioned above may contain electronic evidence to include (but not limited to) messages correspondence, websites, digital photographs, videos, and references to other messages or social media accounts, to support charges for production, distribution, possession of child pornography and enticement of a minor, as described in this affidavit.

SEARCH METHODOLOGY TO BE EMPLOYED REGARDING ELECTRONIC DATA

33. In order to ensure that the Affiant searches only the account and/or files described in this affidavit and application for search warrant, this affidavit and application for search warrants seeks authorization to permit employees of Facebook, Inc. to assist the FBI in the execution of this warrant. To further ensure that the Affiant searches on the account and/or files described in this affidavit, the following procedures will be implemented:

a. In light of Facebook Inc.'s corporate policy and due to the technical nature of this search, it is the Affiant's intention to upload the search warrant to Facebook Inc.'s Law Enforcement portal and request that they actually conduct the search.

b. In order to minimize any disruption of computer service to innocent third parties, the Affiant shall permit Facebook Inc., as custodian of the computer files described in

this affidavit, to locate the files, copy them onto removable electronic storage media or print them out as paper copies, and deliver the copies to the Affiant who need not be present during this process. Facebook Inc. employees will create an exact duplicate of the account and files described in this affidavit.

c. Facebook Inc. employees will provide the exact duplicate in electronic form of the account and files described in this affidavit and all information stored in the account and files to the Affiant.

d. The Affiant and other agents of the Oklahoma City Division of the FBI, or other law enforcement personnel, will thereafter review the information for evidence of violations mentioned herein.

e. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

34. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. §§ 2711, 2703(a), 2703(b)(1)(A) & 2703(c)(1)(A).

CONCLUSION

35. Based on the foregoing, there is probable cause to believe that the search of the SUBJECT ACCOUNT may reveal electronic evidence to include (but not limited to) message correspondence, digital photographs, and videos to support charges for production, distribution, possession of child pornography and coercion and enticement as described in this affidavit.

36. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These

documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation and it is believed that if the individual utilizing the username **saul.frias.14** became aware of federal involvement, he would take steps to destroy electronic media such as computers or cell phones that contain evidence related to the above described offenses. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

Special Agent Jonathan Clark
Federal Bureau of Investigation

Subscribed and sworn to me this 11th day of May, 2016.

KIMBERLY E. WEST
United States Magistrate Judge